2005-001742

MINISTÈRE DE LA DÉFENSE

LES MICRO-ONDES DE FORTE PUISSANCE ET ULB

SITUATION ACTUELLE ET EVOLUTION

Jean-Pierre Percaille

DET/SCET/CEG

DGA

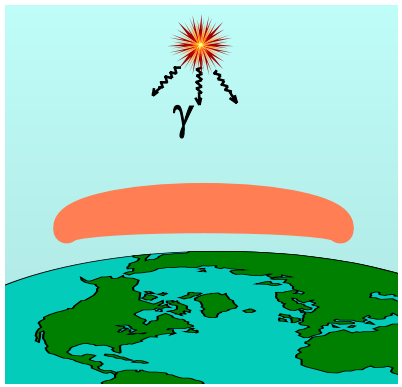
LES MICRO-ONDES DE FORTE PUISSANCE ET ULB

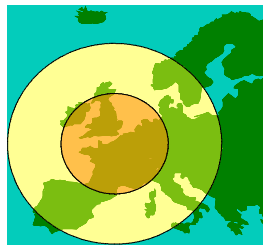
- Généralités
- Types de menaces
- Vulnérabilité
- Potentialité (armes), risques (cibles)
- Evolution

Généralités : Agressions EM

Agressions militaires (intentionnelles)

- IEMN-HA





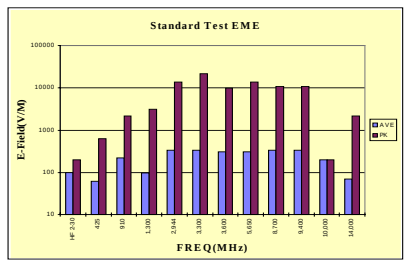
MFP-ULB

Environnements naturels

- Foudre
- DES

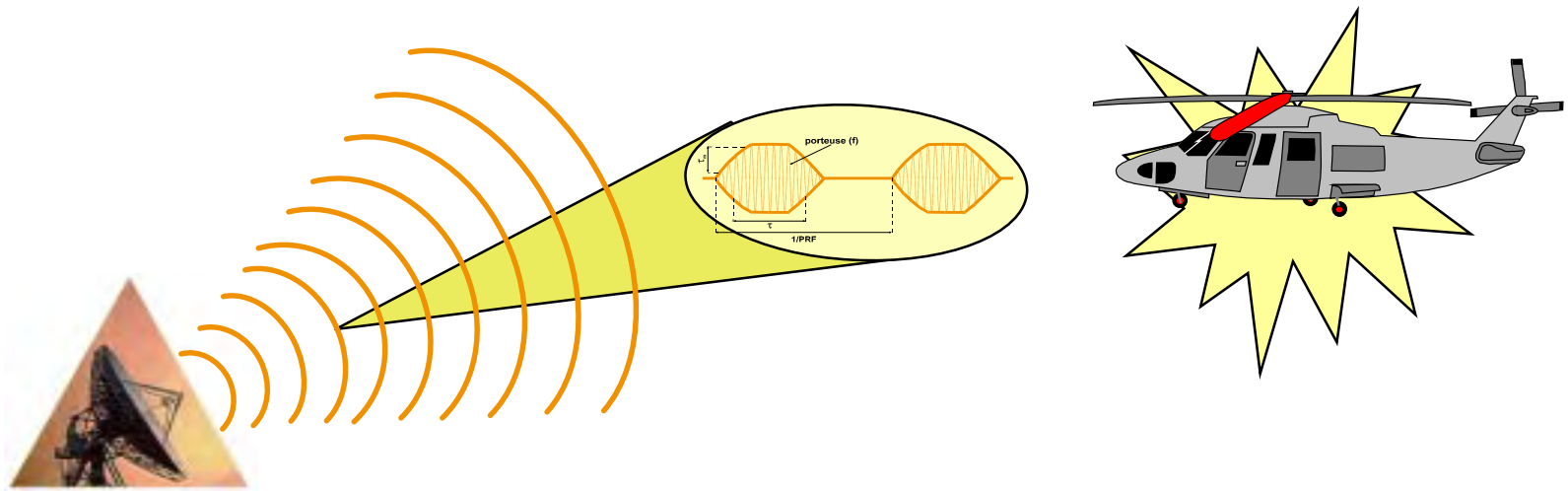
Environnements EM induisant des agressions non intentionnelles

- CEM : Champs forts et radio radar



Généralités : MFP-ULB

Génération d ’une onde sur un système cible susceptible de conduire à un échec de la mission



Données d’entrée

Technologie des sources

Optimisation

Vulnérabilité des systèmes

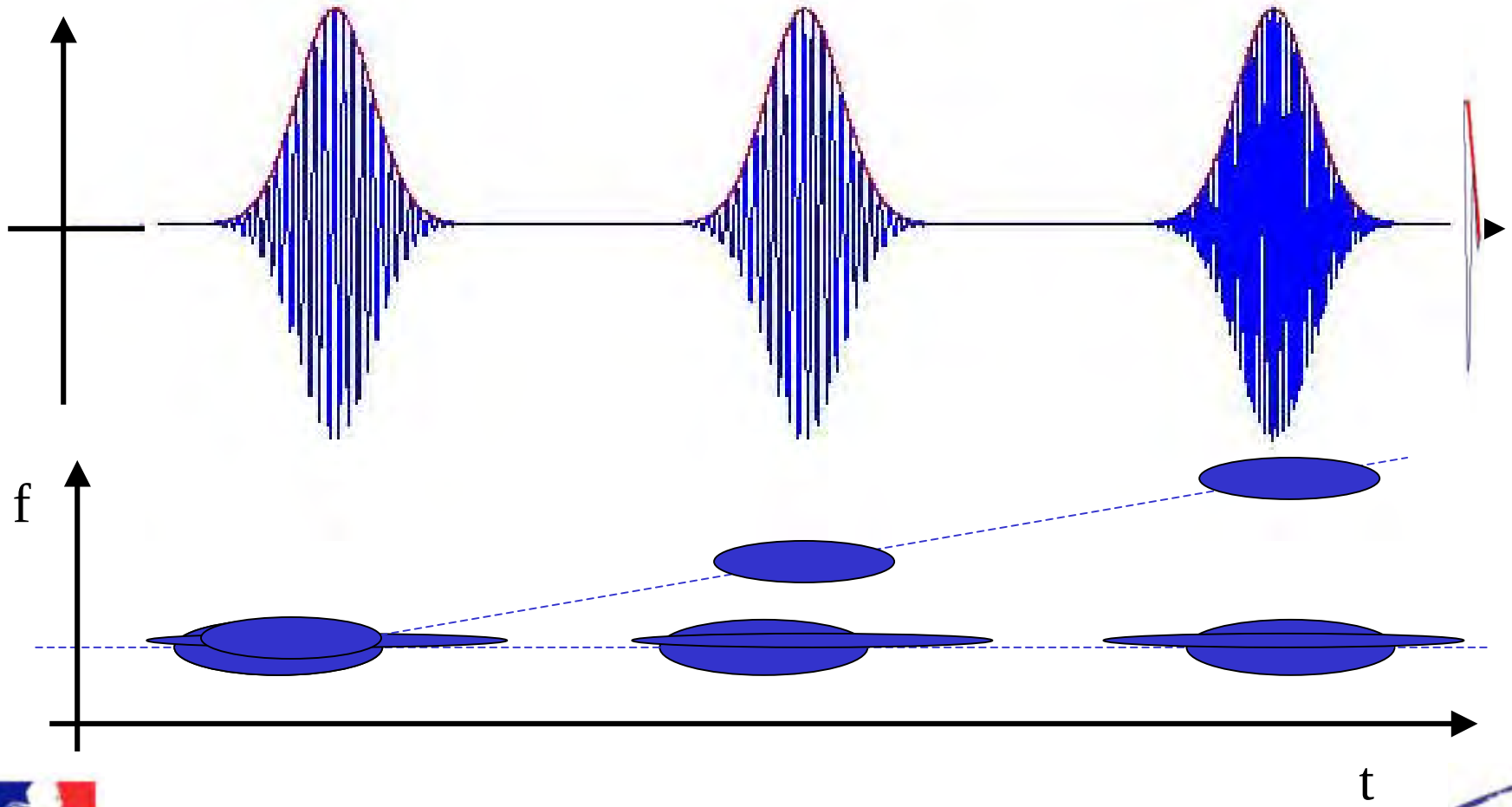
Types de menace :Des MFP aux IEMI

- A l ’origine
  - Micro-onde GHz --->10 ’s de GHz
  - Forte puissance : Source classe GW
  - Durée 100 ’s ns
- IEMI (Impulsions ElectroMagnétiques intentionnelles)
  - MFP mais aussi ...
  - Ultra large bande
  - Sinusoïdale amortie basse fréquence (100 - 300MHz)
  - Moyenne (faible) puissance & longue durée

Diversité des formes : famille bande étroite

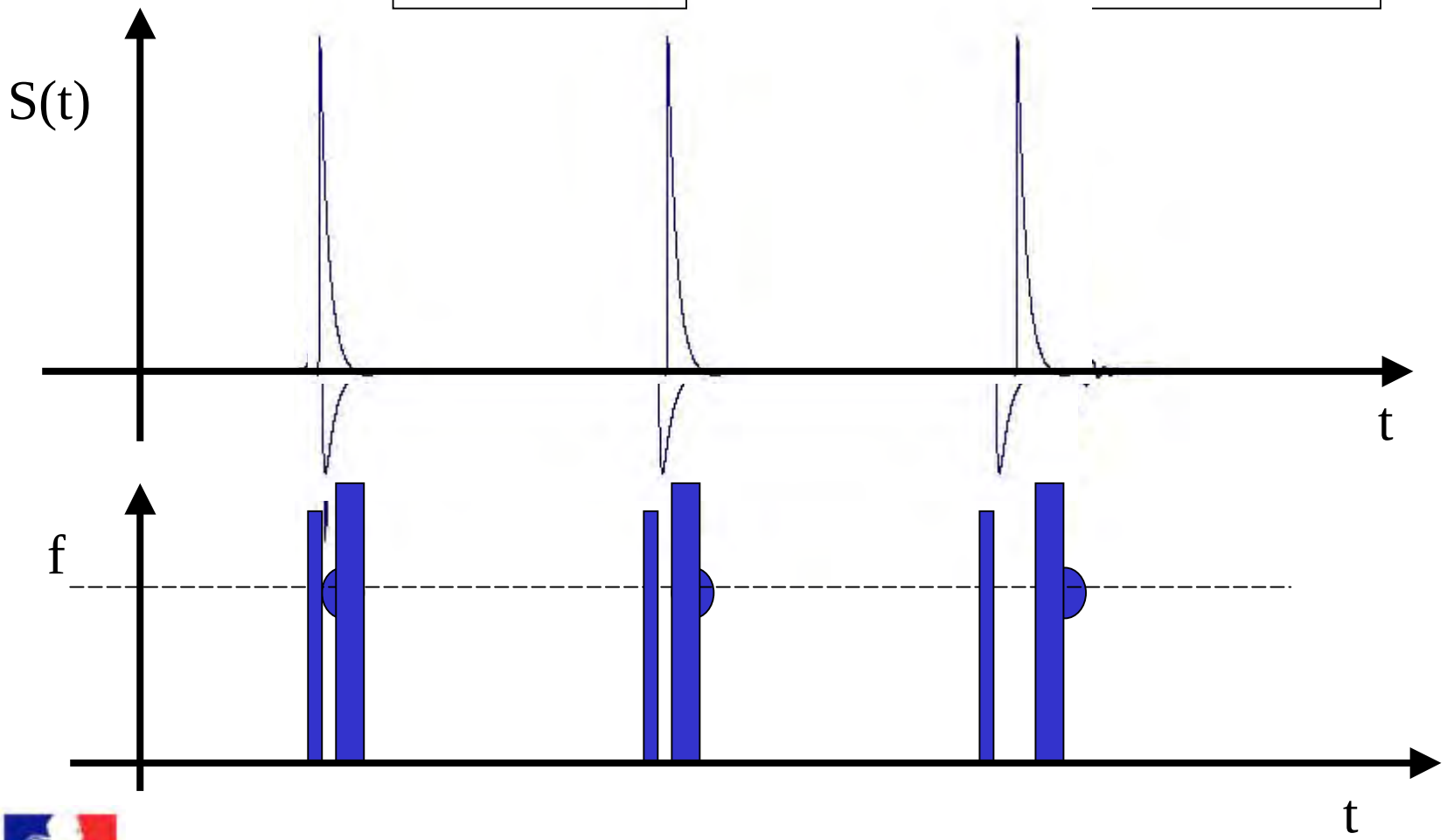
M

Répétitive et agile en fréquen

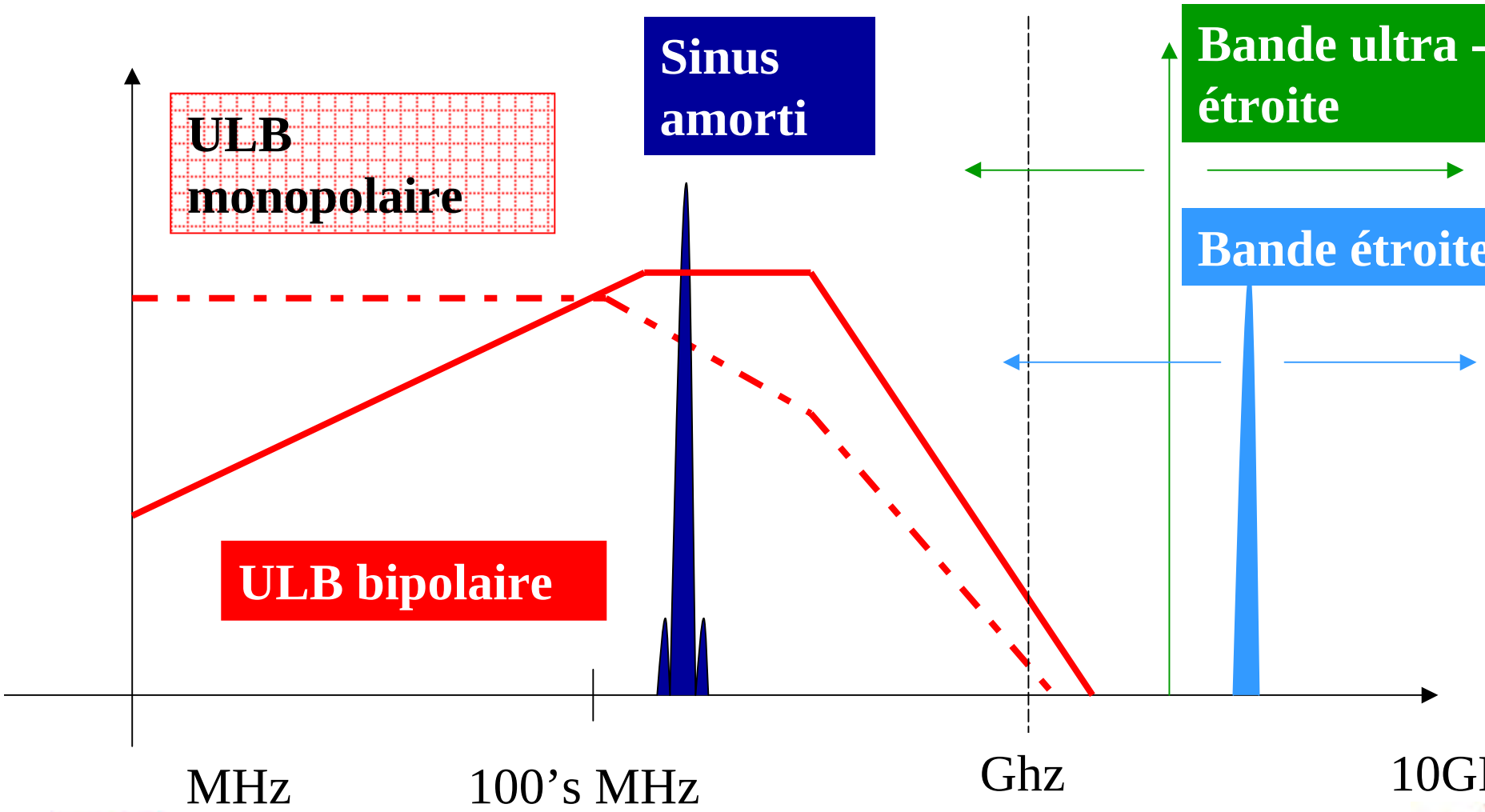


Diversité des formes :famille ULB

Uni-polaire | Bi-polaire | Sinus-amorti



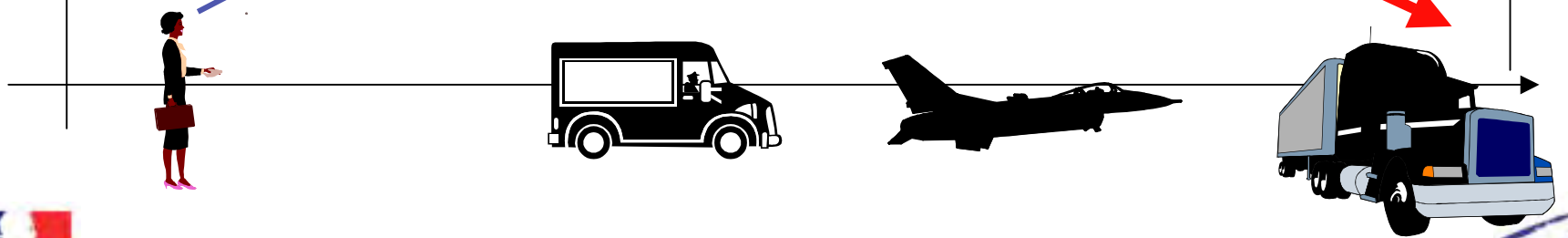
Diversité des formes : Spectre



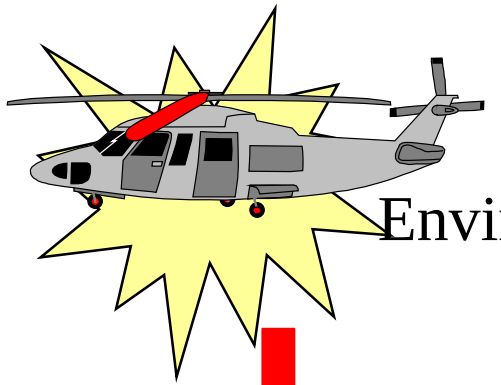
Diversité des volumes (concept d ’emploi)

Discrétion

Energie embarquée

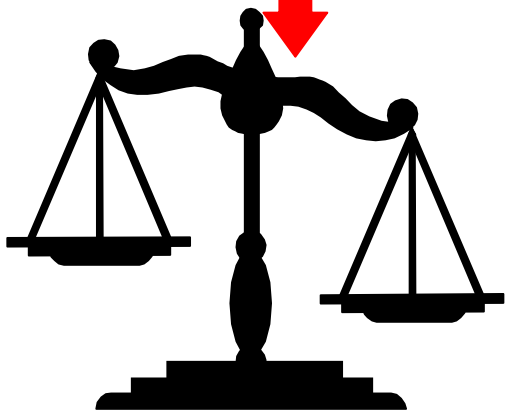


Vulnérabilité des systèmes



Environnement EM

Susceptibilité



Couplage

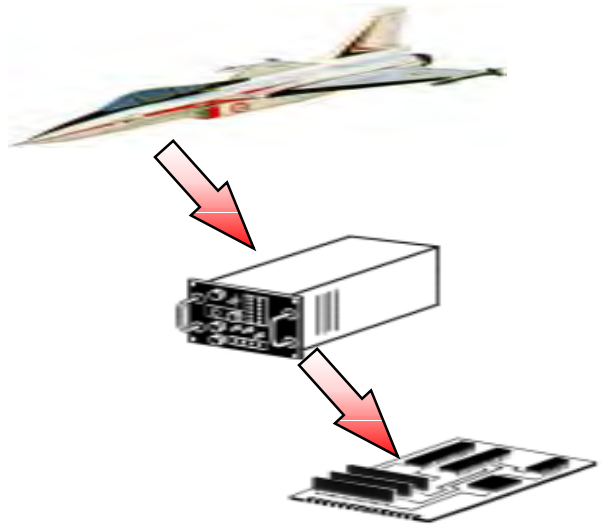
Les modes de couplage

Front-door : Couplage direct par les accès hyperfréquences

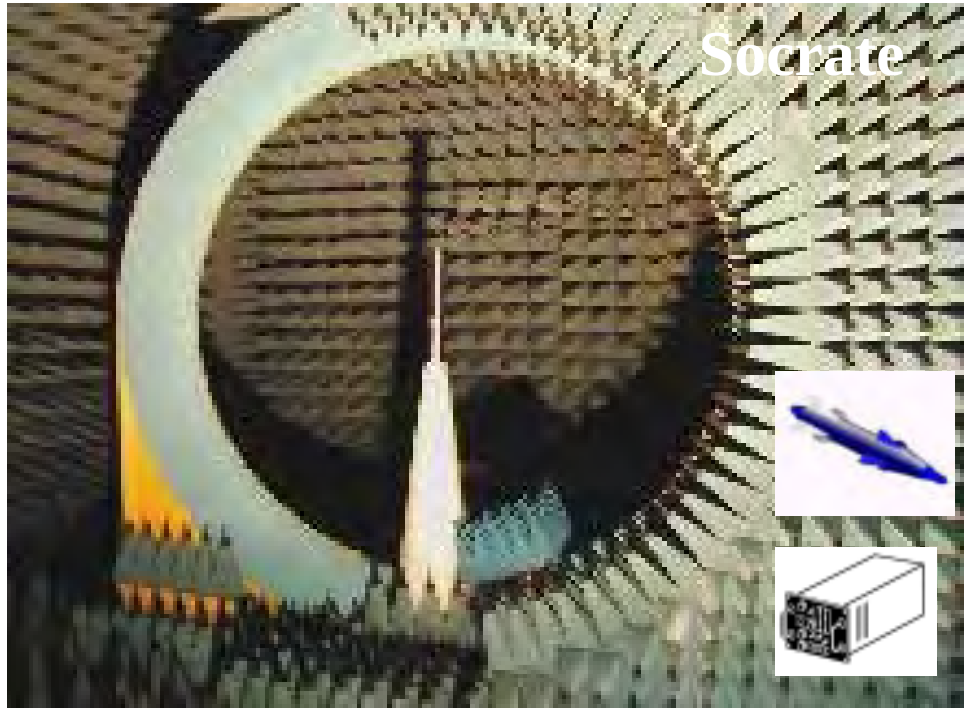
-->Dans la bande

--> Hors bande

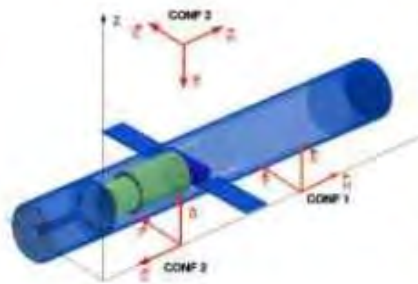
Back-door :Couplage indirect par les défauts de faradisation - blindage

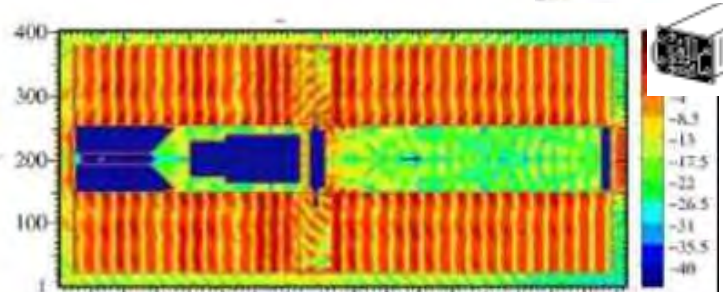


Moyens d ’études de couplage



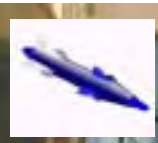
Code 3D, modèle analytique





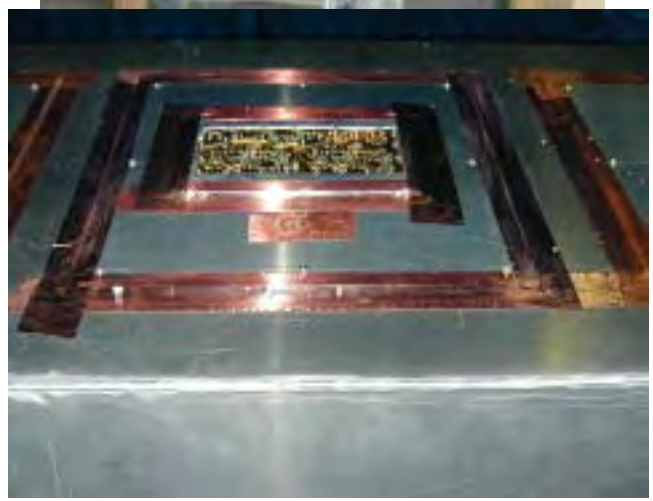
Moyens d ’études de susceptibilité

Hyperion



Chambre anéchoïde & reverbérante

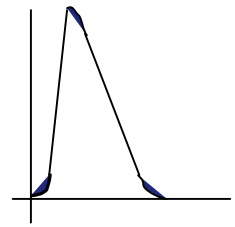
Guide et essais cartes



Moyens d'études de couplage et de susceptibilité ULB

Sinusoïde amortie

ULB

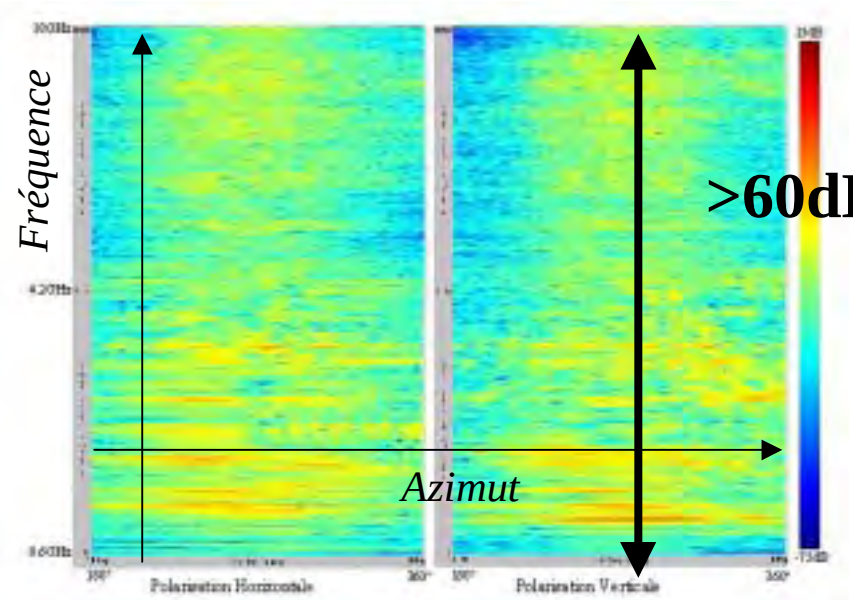


Vulnérabilité / Efficacité

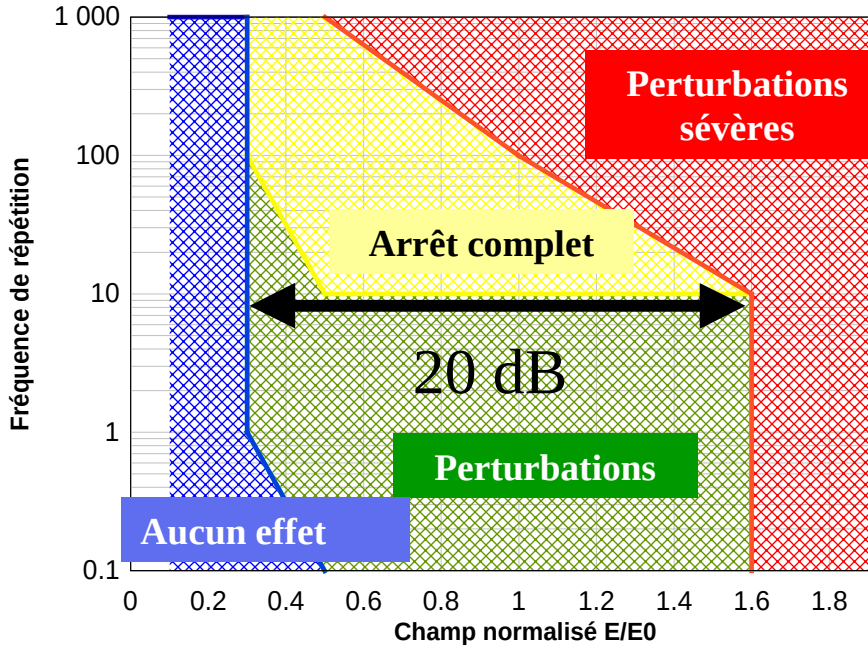
Back-door :

Grande variabilité en couplage & en susceptibilité

Exemple : Résultat ETARCOS



Equipements standards



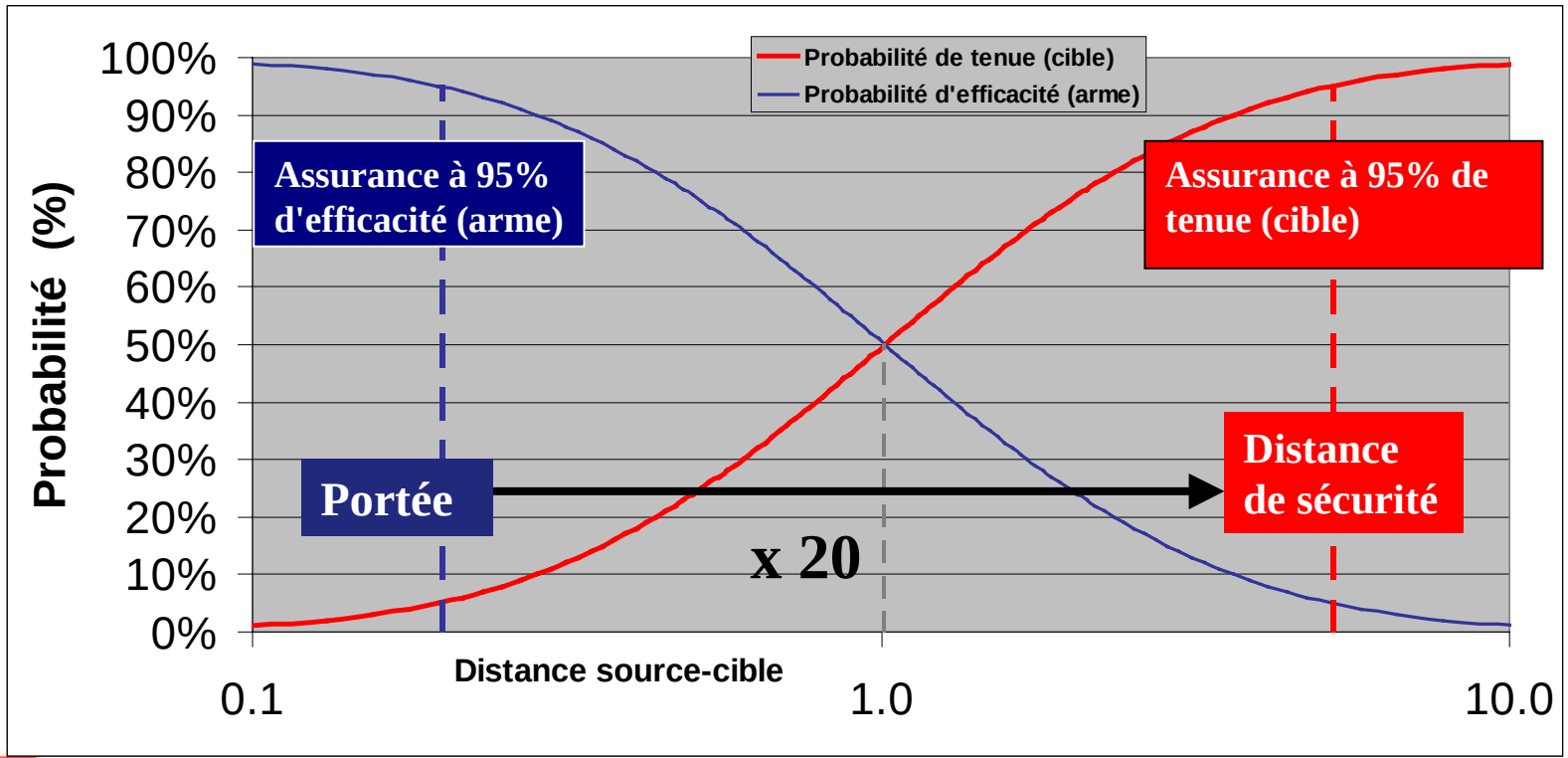
Vulnérabilité / Efficacité IEMI

Exploitation back-door

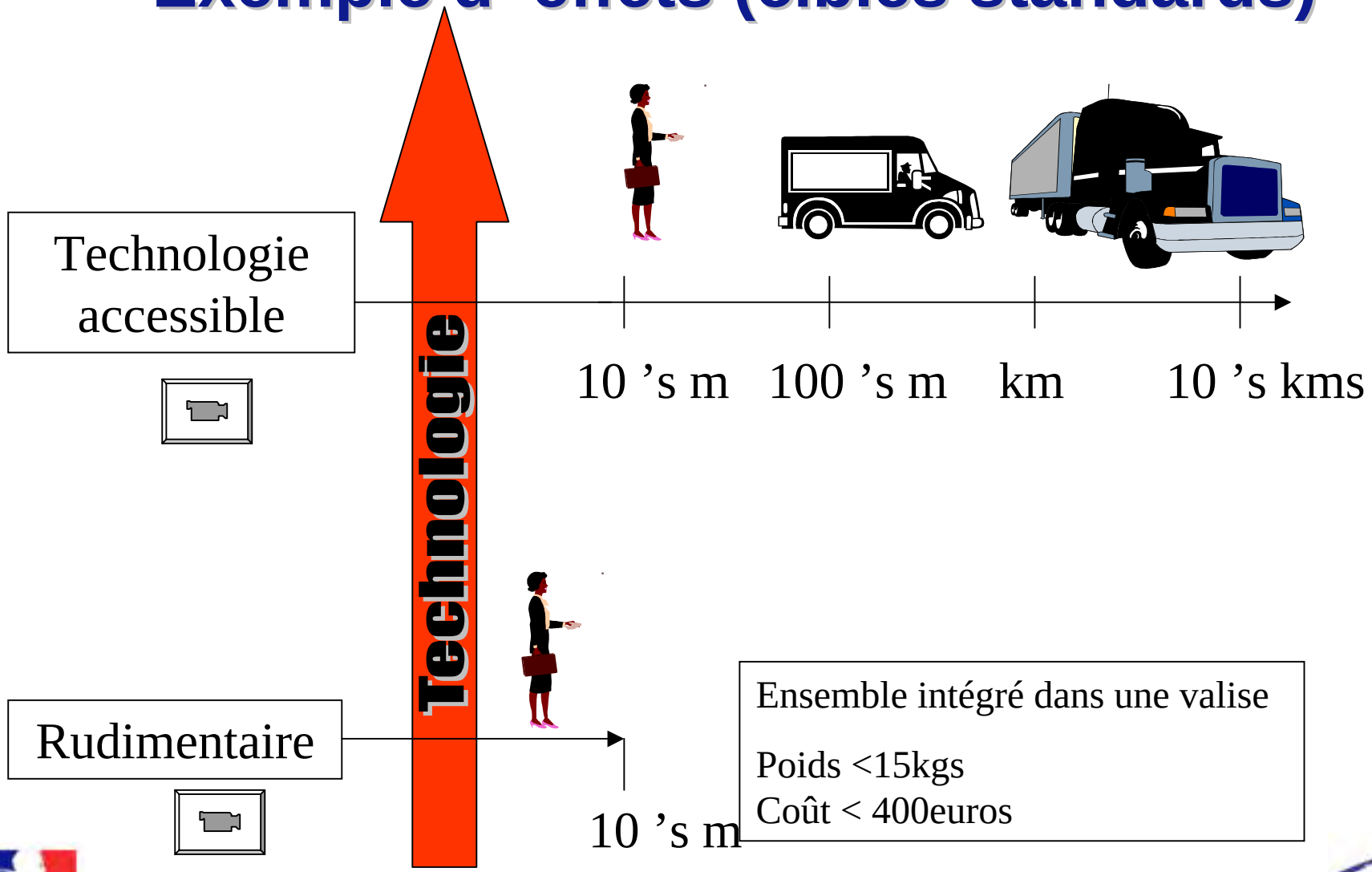
→

Une grandeur opérationnelle

distance source-cible



Exemple d ’effets (cibles standards)



Conclusion (1) : Vulnérabilité acquis et évolution sur la technologie

- Efficacité (cible connue) >> Efficacité (générique)

- La puissance n ’est pas forcément le paramètre prépondérant (formes d ’ondes, fréquence de répétition, agilité, durée, …)

- Des armes de technologies rudimentaires peuvent s ’avérer efficaces

Orientations vers des armes dédiées à des familles de cibles, prise en compte de l ’ensemble des IEMI

Conclusion (2) : Vulnérabilité acquis et évolution sur la protection

- Vulnérabilité système cible (distance de sûreté) ≠ Efficacité arme (portée)

- Nombres de systèmes d ’armes se sont avérés vulnérables à une forme IEMI

La nécessité de protéger les systèmes et installations vis à vis des IEMI* paraît indispensable.

(*y compris celles issues de technologies rudimentaires)